KANTAR

# Retail under siege: How cyber crime is raising the stakes

## Key issues and impact on trade

Paida Mugudubi
Head of Retail Insights (EMEA & APAC)

Howard Lake
Sr. Content & Insights Manager, EMEA

May 2025
REGION: GLOBAL



# Headlines

## 1 The issue

Cybercrimes are on the increase with the scale and impact of the damages amplifying across all businesses. AI is accelerating the issue with 91% of security experts saying they expect a significant rise in AI-driven threats over the next three years. Marks & Spencer (M&S), Cooperative Group and Harrods are the latest British retailers to have experienced cyber attacks.

## 2 Scale of the problem

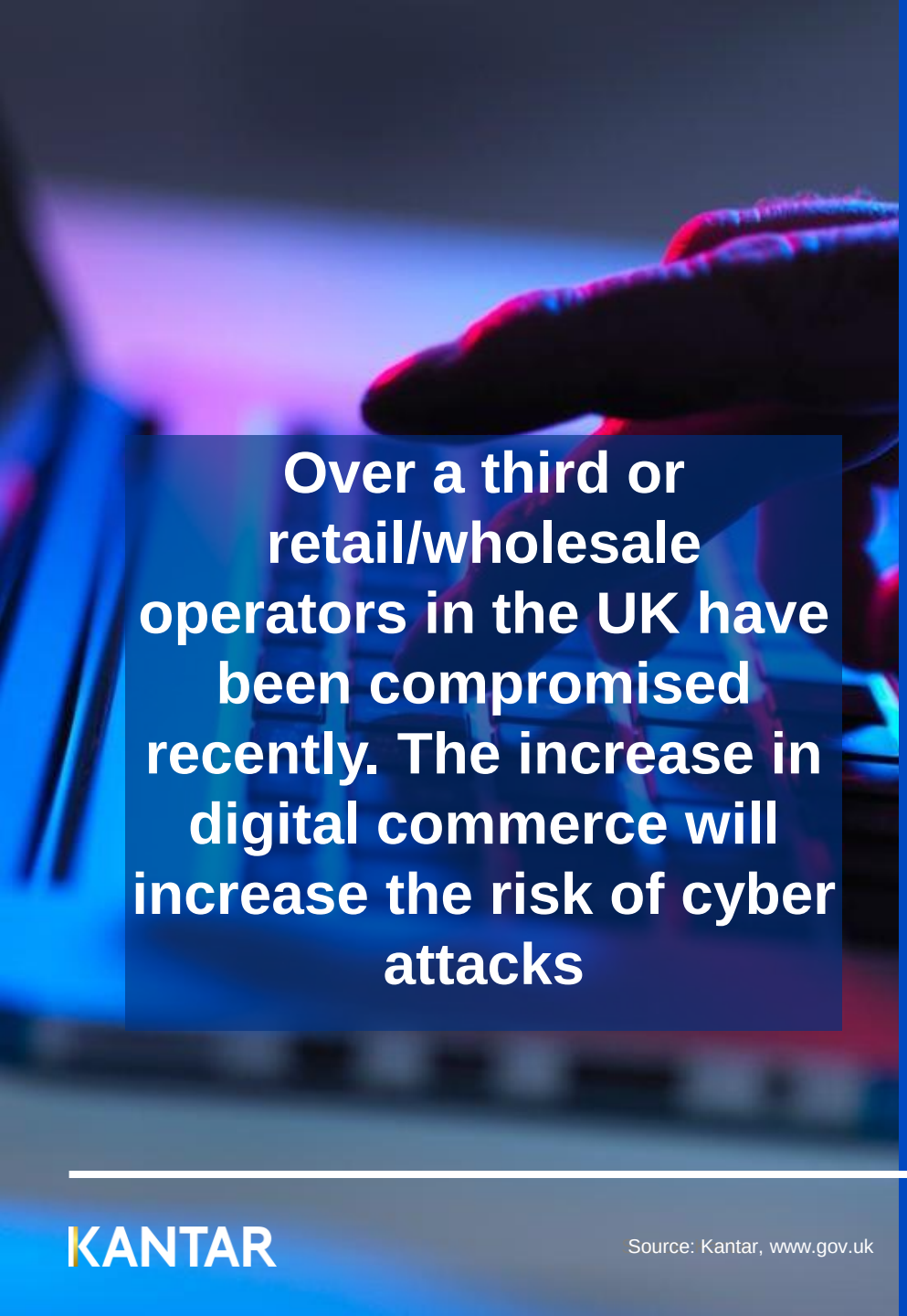
Globally the cost of cybercrime will reach USD13.8 trillion by 2028; an increase of 50% from 2024. According to a PwC survey, 42% of companies generating more than USD1 billion annually have faced attacks in the past two years. Cyberattacks have cost UK businesses an estimated GBP44 billion (USD55.08 billion) in lost revenue over the past five years. On average, firms lose 1.9% of their revenue to cyber incidents, with those earning over GBP100 million annually at greatest risk. The recent attack on M&S has reportedly cost the retailer over GBP800 million

## 3 Finding solutions for a shape shifting challenge

The EuroCIS 2025 trade fair held in Düsseldorf, Germany in February 2025 had a strong focus on IT security. For the first time, the event featured a dedicated space for IT security with exhibitors presenting solutions to safeguard customer data, prevent cyberattacks, and manage supply chain risks. The UK government through its National Cyber Security Centre (NCSC) has weighed on recent UK attack, urging businesses to follow its advice and step up vigilance. Long-term, staying ahead of how AI is being weaponized and greater industry collaboration to find solutions should help build stronger defences for a continuously shifting threat.

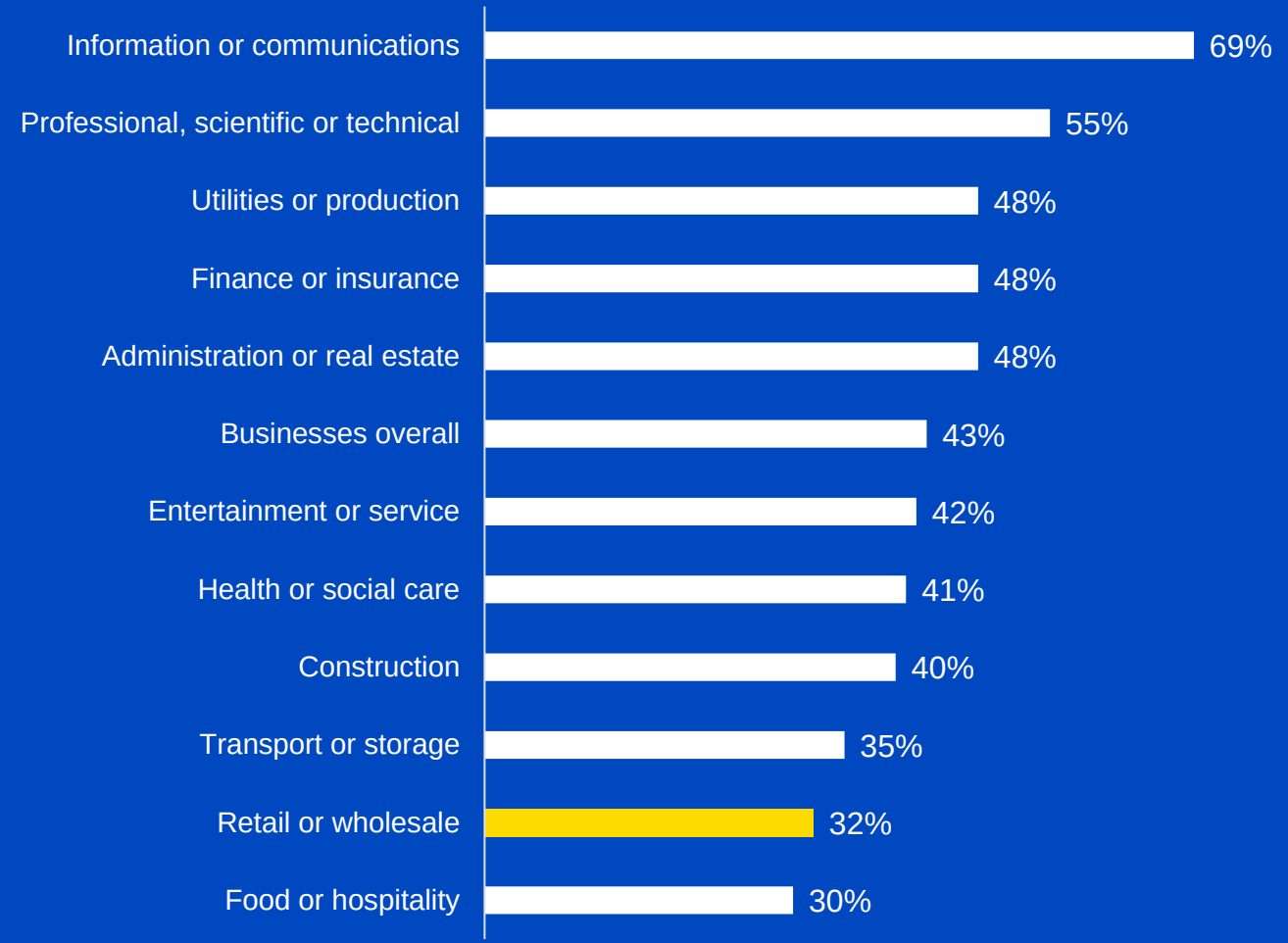
KANTAR

Source: Kantar, Howden, PWC



**Over a third or retail/wholesale operators in the UK have been compromised recently. The increase in digital commerce will increase the risk of cyber attacks**

Percentage of businesses in the **UK** that have identified breaches or attacks in the last 12 months by Sector




KANTAR

Source: Kantar, www.gov.uk

# The weaponization of AI and more access points increases risks of cybercrimes

Criminals are **increasingly using AI** to:

- Craft more convincing phishing attacks
- Quickly identify vulnerabilities
- Launch highly targeted operations

Retailers are **expanding their digital footprints**

**Long value chains** means more **access points**

**More Cloud, more remote work**, more interconnected systems

KANTAR

Source: Kantar, CEBR, Adyen, TC3

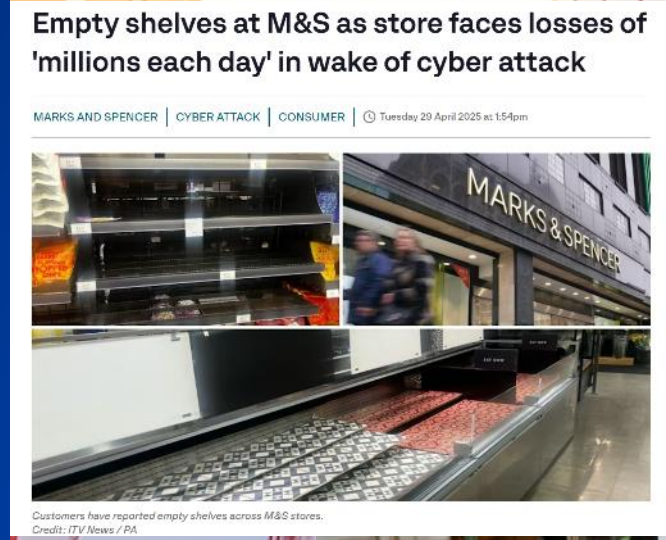
# M&S cyber attack wipes millions off its market value

**April 2025:** Marks and Spencer (M&S) grappled with a serious cyber attack that forced the retailer to suspend online orders, disrupted in-store operations, and blocked its remote staff from working on its system.

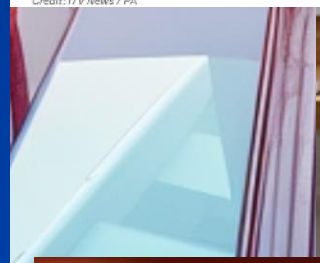
- More than a week to resolve
- Suspended online orders
- ~200 agency workers at its main distribution centre were asked to stay home
- Shares plunged 6.9% over the seven days to 29 April, and around GBP700 million has been wiped off the company's market value.

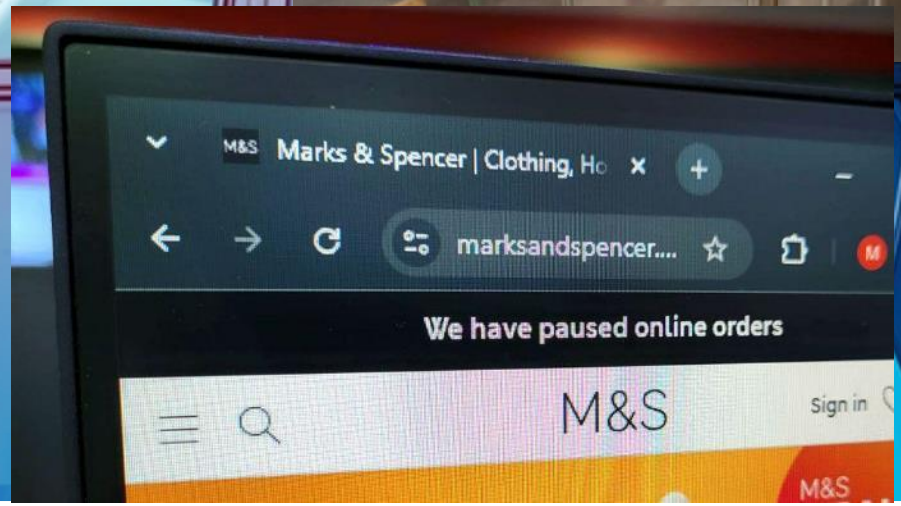
*"I would suggest that there is a high level of confidence this is a ransomware-style event.* ***I describe these like a digital bomb has gone off.*** *So recovering from them is often both technically and logistically challenging"*

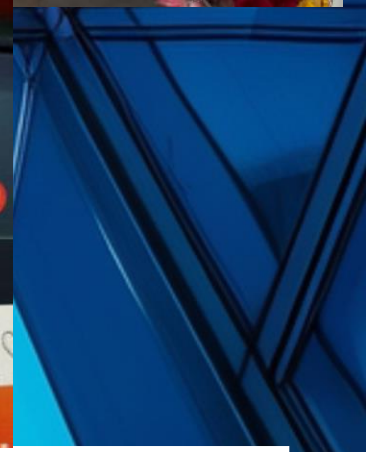
Dan Cart, Cyber Expert at BCS











Source: Kantar, BBC, Money Week, ITV

# Retailers are tackling a constantly shifting and evolving problem


April 2025: M&S ransomware attack


April 2025: Co-Op systems hacked


April 2025: Harrods systems breach


Nov 2024: Ahold Delhaize data systems breach

BlueYonder

Nov 2024: Blue Yonder ransomware attack hits Sainsbury's, Morrisons etc.


Nov 2024: Auchan sees data breach of 500,000 loyalty members' information.

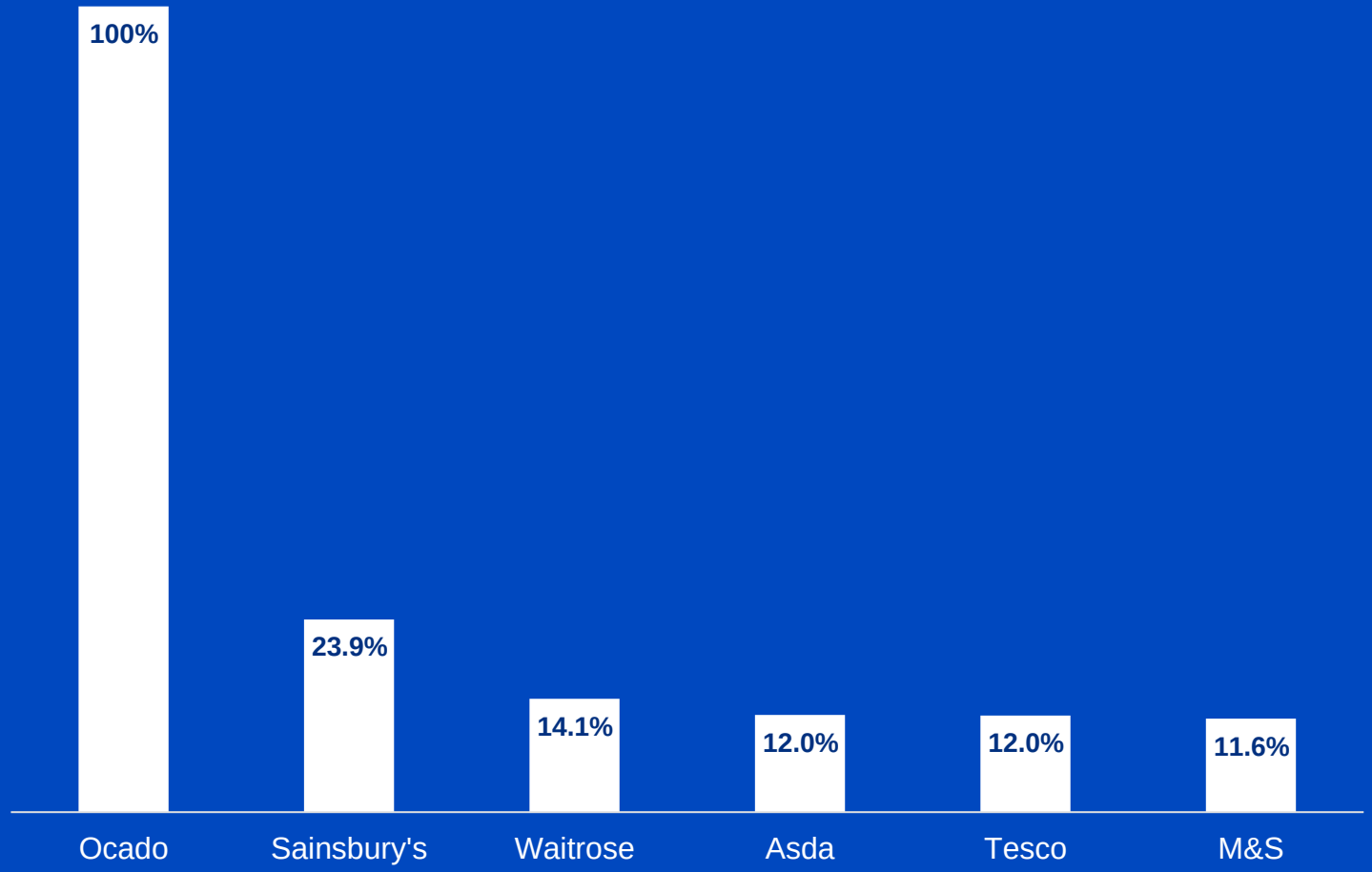
KANTAR

Source: Kantar, FICO, Company media

The risk plays out as a partial or total disruption to online ordering as well as logistics that replenish shelves in stores

Losing viability of channel that contributes +10% of sales even if for a few days is material

## UK Contribution to Online Sales, 2024e (%)




Source: Kantar

# 7

things to know



1. Cyber risk is increasing across businesses and damages will multiply. **A 50% increase in damages** is projected globally from 2024 t0 2028
2. **AI proliferation is a double-edged sword** – weaponized to implement attacks quickly and dynamically but also leveraged for solution development
3. The continued **growth of digital** commerce opens the **scope for more breaches** over the long term
4. **Long supply chains** also proliferates **access points** of attacks across retail value chains
5. Brands/suppliers should invest in **avoiding being the weakest link** that enables an attack on their retail partners
6. Fragmented systems across the retail value chain create multiple entry points for attacks, risking major system breaches. This highlights the **need for industry-wide investment** in stronger, unified defences.
7. Governments also need to **step up their national cybersecurity strategies** and promote better public-private collaboration

KANTAR

Source: Kantar

**Paida Mugudubi**
Head of Retail Insights
paida.mugudubi@kantar.com

**Howard Lake**
Senior Manager, Global Retailer Insights Content
Howard.lake@kantar.com

Kantar | 30 Stamford St, London SE1 9LQ | www.kantar.com

111 Huntington Ave., 20th Floor, Boston, MA 02199

## Notice



## Disclaimers

The analyses and conclusions presented in these materials represent the opinions of Kantar Consulting. The views expressed do not necessarily reflect the views of the management of the retailer(s) under discussion. These materials are not endorsed or otherwise supported by the management of any of the companies or organizations discussed herein.